

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-050956

(43)Date of publication of application : 15.02.2002

(51)Int.Cl.

H03K 19/173

G06F 1/00

H04L 9/10

(21)Application number : 2000-212303

(71)Applicant : SUN MICROSYST INC

(22)Date of filing : 13.07.2000

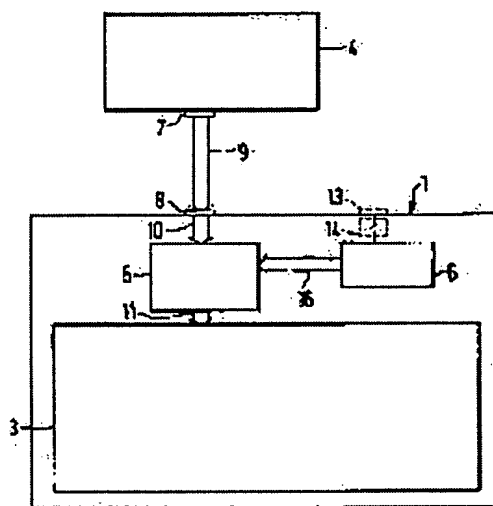
(72)Inventor : GARNETT PAUL JEFFREY

(54) FIELD PROGRAMMABLE GATE ARRAY

(57)Abstract:

PROBLEM TO BE SOLVED: To prevent the data structure from being intercepted upon reconfiguration of volatile FPGA.

SOLUTION: For example, upon power source making, ciphered configuration data are fed to the input terminal of FPGA. In FPGA, the configuration data are first decoded by decoding algorithm embedded in the logic. This algorithm uses nonvolatile memory in FPGA, such as decoding key stored in an EEPROM, as an operand. The decoded configuration data are distributed to volatile function part in FPGA in conventional way. According to this design, even when the streams of configuration data which are transmitted from the external memory to FPGA upon reconfiguration are intercepted, the intercepting part can obtain only ciphered configuration data. Thus, this design can improve security, protecting intellectual property of commercial value and secret information, consisting of non-ciphered configuration data.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2002-50956

(P2002-50956A)

(43) 公開日 平成14年2月15日 (2002.2.15)

(51) Int.Cl. ⁷	識別記号	F I	テマコード [*] (参考)
H 0 3 K 19/173	1 0 1	H 0 3 K 19/173	1 0 1 5 B 0 7 6
G 0 6 F 1/00		G 0 6 F 9/06	6 6 0 L 5 J 0 4 2
H 0 4 L 9/10		H 0 4 L 9/00	6 2 1 A 5 J 1 0 4

審査請求 未請求 請求項の数23 O L (全 10 頁)

(21) 出願番号 特願2000-212303 (P2000-212303)

(22) 出願日 平成12年7月13日 (2000.7.13)

(71) 出願人 591064003

サン・マイクロシステムズ・インコーポレ
ーテッドSUN MICROSYSTEMS, IN
CORPORATEDアメリカ合衆国 94303 カリフォルニア
州・パロ アルト・サン アントニオ ロ
ード・901

(74) 代理人 100064621

弁理士 山川 政樹

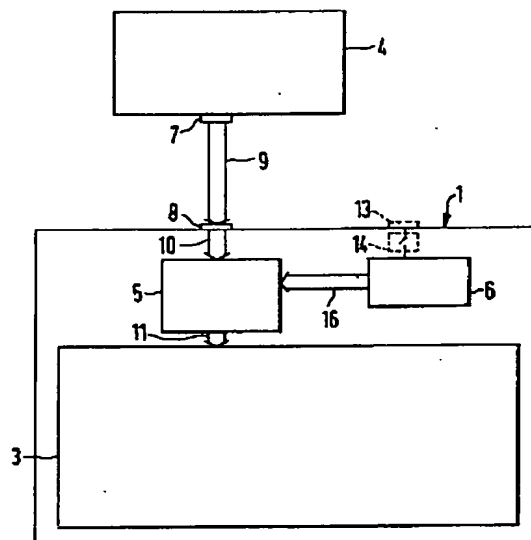
最終頁に続く

(54) 【発明の名称】 フィールド・プログラマブル・ゲート・アレイ

(57) 【要約】

【課題】 揮発性 F P G A を再構成するときにそのデータ構造を傍受できないようにする。

【解決手段】 例えば電源投入時に、暗号化された構成データが F P G A の入力端子に供給される。F P G A 中で、構成データはまず、論理に埋め込まれた復号アルゴリズムによって復号される。このアルゴリズムは、F P G A 中の不揮発性メモリ、例えば E E P R O M に記憶された復号鍵をオペランドとして使用する。復号された構成データは、従来の方式で F P G A の揮発性機能部分に配送される。この設計によれば、再構成時に外部メモリから F P G A に転送される構成データのストリームを傍受しても、暗号化された構成データしか得られない。そのため、この設計は、暗号化されない構成データで形成された商業的価値のある知的財産および機密情報が失われることがないような安全性の向上をもたらす。



1

【特許請求の範囲】

【請求項 1】 (a) 構成可能論理構造を有する機能部分と、

(b) 前記機能部分を構成する構成データを受け取る入力端子と、

(c) 前記入力端子と前記機能部分との間に配置され、前記入力端子で受け取った前記構成データに復号プロセスを適用し、復号した前記構成データを、前記機能部分を構成するために機能部分へ中継するように構成される復号回路とを含むフィールド・プログラマブル・ゲート・アレイ。 10

【請求項 2】 前記復号回路が復号鍵記憶域および復号論理を含み、前記復号論理に、前記復号鍵記憶域から取り出せる復号鍵をアルゴリズムのオペランドとして使用して前記構成データに適用できる復号アルゴリズムが埋め込まれている請求項 1 に記載のフィールド・プログラマブル・ゲート・アレイ。

【請求項 3】 前記復号鍵記憶域が不揮発性素子で形成される請求項 2 に記載のフィールド・プログラマブル・ゲート・アレイ。 20

【請求項 4】 前記不揮発性素子が、前記フィールド・プログラマブル・ゲート・アレイの方々に物理的に分散して配置されている請求項 3 に記載のフィールド・プログラマブル・ゲート・アレイ。

【請求項 5】 前記不揮発性素子が、EEPROM素子、フラッシュPROM素子、UV-EPROM素子、OTPROM素子、ヒューズブル・リンクPROM素子、強誘電体セル、およびレーザ・プログラマブル・ヒューズからなるグループの少なくとも 1 つである請求項 3 に記載のフィールド・プログラマブル・ゲート・アレイ。 30

【請求項 6】 前記ゲート・アレイの前記機能部分が揮発性素子で形成される請求項 1 に記載のフィールド・プログラマブル・ゲート・アレイ。

【請求項 7】 前記揮発性素子がSRAM素子である請求項 6 に記載のフィールド・プログラマブル・ゲート・アレイ。

【請求項 8】 前記復号回路が不揮発性素子で形成され、前記ゲート・アレイの前記機能部分が揮発性素子で形成される請求項 1 に記載のフィールド・プログラマブル・ゲート・アレイ。 40

【請求項 9】 前記不揮発性素子が前記揮発性素子の間に分散して配置される請求項 8 に記載のフィールド・プログラマブル・ゲート・アレイ。

【請求項 10】 前記復号鍵記憶域が不揮発性素子で形成され、前記ゲート・アレイの前記機能部分が揮発性素子で形成される請求項 2 に記載のフィールド・プログラマブル・ゲート・アレイ。

【請求項 11】 前記復号鍵記憶域が不揮発性EEPROM素子で形成され、前記ゲート・アレイの前記機能部 50

2

分が揮発性SRAM素子で形成される請求項 1 に記載のフィールド・プログラマブル・ゲート・アレイ。

【請求項 12】 復号鍵を前記復号鍵記憶域にロードできる鍵入力端子を含む請求項 2 に記載のフィールド・プログラマブル・ゲート・アレイ。

【請求項 13】 外部から加えることのできるディスエーブル化信号の受領により前記復号鍵記憶域への後続の外部通信を閉鎖するよう、不可逆的な変更が前記フィールド・プログラマブル・ゲート・アレイに引き起こされるように構築されるディスエーブル化素子を含む請求項 12 に記載のフィールド・プログラマブル・ゲート・アレイ。

【請求項 14】 (a) 構成データ・セットを入力するステップと、

(b) ユーザ指定の暗号鍵をオペランドとして有する暗号化アルゴリズムを前記構成データ・セットに適用するステップと、

(c) 記録媒体上に前記暗号化した構成データを記憶するステップとを含む、フィールド・プログラマブル・ゲート・アレイ構成データを処理する方法。

【請求項 15】 (d) 前記暗号鍵から復号鍵を生成するステップと、

(e) フィールド・プログラマブル・ゲート・アレイの不揮発性メモリに前記復号鍵を書き込むステップとをさらに含む請求項 14 に記載の方法。

【請求項 16】 (a) 暗号化された構成データをフィールド・プログラマブル・ゲート・アレイに入力するステップと、

(b) 前記暗号化された構成データを前記フィールド・プログラマブル・ゲート・アレイ内で復号するステップと、

(c) 前記フィールド・プログラマブル・ゲート・アレイ内で前記復号した構成データを配信して、前記フィールド・プログラマブル・ゲート・アレイを構成するステップとを含む、フィールド・プログラマブル・ゲート・アレイを再構成する方法。

【請求項 17】 前記復号ステップ (b) が、前記フィールド・プログラマブル・ゲート・アレイ内に不揮発性の形で記憶された復号鍵をアルゴリズムのオペランドとして使用して、前記暗号化された構成データに復号アルゴリズムを適用するステップを含む請求項 16 に記載の方法。

【請求項 18】 前記ステップ (b) で前記復号アルゴリズムがステートフルである請求項 17 に記載の方法。

【請求項 19】 構成可能論理構造を有する機能部分と、前記機能部分を構成する構成データを受け取る入力端子と、前記構成データに復号プロセスを適用して、フィールド・プログラマブル・ゲート・アレイの前記機能部分を構成させために復号した構成データを生成する復号手段とを含むフィールド・プログラマブル・ゲート・

アレイ。

【請求項20】 前記復号手段が、復号鍵を記憶する手段と、前記復号鍵をアルゴリズムのオペランドとして使用して前記構成データに復号アルゴリズムを適用する手段とを含む請求項19に記載のフィールド・プログラマブル・ゲート・アレイ。

【請求項21】 復号された構成データを受け取る入力端子と、デフォルト状態を有する構成可能論理構造であって、それぞれが復号された構成データのセットによって定義される複数のプログラム状態のいずれかにプログラム可能である構成可能論理構造と、前記プログラム状態の1つを定義する復号された構成データのセットを記憶するデータ記憶域とを含むフィールド・プログラマブル・ゲート・アレイであって、前記構成可能論理構造がデフォルト状態で、前記入力端子で受け取った暗号化された構成データを復号するように、かつ、続いて前記構成可能論理構造を前記復号した構成データ・セットによって定義されるプログラム状態に再構成するために対応する復号した構成データ・セットを前記データ記憶域に記憶するように構成されるフィールド・プログラマブル・ゲート・アレイ。

【請求項22】 前記データ記憶域が複数の構成データ保持レジスタを含む請求項21に記載のフィールド・プログラミング・ゲート・アレイ。

【請求項23】 前記構成可能論理構造による復号の完了を検出するように、かつ、前記データ記憶域に記憶された前記構成データを前記構成可能論理構造にロードするために前記データ記憶域をトリガし、それにより前記構成可能論理構造をプログラム状態に再構成するように接続される状態機械を含む請求項21に記載のフィールド・プログラマブル・ゲート・アレイ。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明はフィールド・プログラマブル・ゲート・アレイに関し、限定しないが特に、揮発性フィールド・プログラマブル・ゲート・アレイに関する。

【0002】

【従来の技術】フィールド・プログラマブル・ゲート・アレイ（FPGA）は、論理構造を含む機能部分を含み、その構成は、設計段階で、関係するアプリケーションに対して特定される構成データによって決められる状態にプログラム可能であり、FPGAにロード可能である。

【0003】揮発性技術に基づくFPGAは、広く使用されている。AlteraコーポレーションおよびXilinx社の各社が、この分野で活動的である。このような揮発性FPGAは、電力が除去されるときにその構成を失う。したがって揮発性FPGAは、電源投入時に、外部で保持される構成データを再ロードすることに

よって再構成される。この機能を実行するために、揮発性FPGAには、それぞれの構成データをFPGAの機能部分内の適切な素子にルーティングするための回路が備わっている。

【0004】電源投入時に構成データを再ロードするとき、外部構成データ記憶装置とFPGAとの間のデータ・ストリームを傍受して、FPGAが構成されている通りの構成データを観察することは比較的簡単であろう。さらに、プログラムされたFPGAの未許可リバース・エンジニアリングが、傍受した構成データを利用する可能性もある。

【0005】第1の可能性は、公開市場でプログラムされていないFPGAを入手して、傍受した構成データでそれらをプログラムすることであろう。

【0006】第2の可能性は、構成データからFPGAの設計を論理レベルでリバース・エンジニアリングし、かつ、傍受した構成データまたは他の構成データでプログラムされた設計でFPGAを製造することである。これは、傍受した構成データとその結果得られるFPGAの構成との関係が分かれば可能となる。次いで、例えば元のFPGA論理の未許可リバース・エンジニアリングを他の設計の足掛かりとして使用するためや、その設計が元のFPGAからのリバース・エンジニアリングによって得られたものであることを隠すために、リバース・エンジニアリングしたFPGA設計に修正を加えることも可能である。

【0007】第3の可能性は、構成データとその結果得られるFPGAの構成との関係が分からない場合に採用できるが、スライス・アンド・スキャン方法、または他のハードウェア・クローニング技術を使用してFPGAをハードウェア・レベルでリバース・エンジニアリングすることであろう。

【0008】したがって、おそらくかなりの期間にわたり設計者のチームを伴って元の設計作業の後に生み出されたかも知れない商業的価値のある構成データが未許可複製される潜在性がある。さらに、FPGA構成プロセスの間の未許可の傍受で得られた構成データの使用により、FPGAハードウェアが論理レベルで未許可リバース・エンジニアリングされる潜在性もある。

【0009】

【発明が解決しようとする課題】本発明の目的は、揮発性フィールド・プログラマブル・ゲート・アレイ（FPGA）を揮発後に再構成させるとき、外部から送られてきた構成用データを傍受されてもその内容を分らないようにする。

【0010】

【課題を解決するための手段】本発明による特定の好ましい態様は、添付の独立クレームおよび従属クレームに述べる。従属クレームの特徴は、適切に、クレームに明示的に述べる特徴以外の組み合わせで、独立クレームの

5

特徴と組み合わせることができる。

【0011】本発明の第1の態様によれば、暗号化された構成データを受け取るように構成され、再構成中、例えば電源投入時に受け取った暗号化された構成データに作用してそれを復号するための復号論理をその入力側に有するフィールド・プログラマブル・ゲート・アレイが提供される。復号化された構成データは、次いで、フィールド・プログラマブル・ゲート・アレイ内で従来方式で処理される。すなわち、フィールド・プログラマブル・ゲート・アレイの機能部分の論理構造を構成するよう10に配信される。

【0012】本発明の一実施態様では、復号論理が、FPGA内に記憶された復号鍵にアクセスする。次いで復号アルゴリズムが、この鍵をオペランドとして使用する。復号アルゴリズムは、ステートレスであるよりもステートフルである方が好ましい。ステートフルなアルゴリズムは、標準的なリニア・フィードバック・シフト・レジスタ(LFSR)設計に基づくハードウェア中で実現することができる。通常、鍵メモリは、不揮発性記憶素子、例えばEEPROMで形成され、ゲート・アレイ20の機能部分は、揮発性素子、例えばSRAMで形成される。鍵サイズは、通常およそ1キロビットまたはそれ以上とすることができる。このサイズは、現在のコード・クラッキング技術を顧慮した所望のデータ安全性レベルを提供するように選択される。いくつかのアプリケーションには、より小さいサイズ、例えば64ビット、128ビット、または256ビットでも適する場合がある。

【0013】鍵メモリが一般に、FPGAの機能部分のゲート・アレイに比べてFPGAの小部分しか形成しないことになるため、鍵メモリは、歩留りに有利な比較的大きい機構サイズのハードウェア中で実現することが30できる。

【0014】本発明の第2の態様によれば、フィールド・プログラマブル・ゲート・アレイ構成データを処理する方法が提供される。この方法は、構成データを入力すること、構成データを暗号化すること、および暗号化した構成データを構成データ・メモリに、または続いて構成データ・メモリにロードするために中間記録媒体に記憶することを含む。暗号化は、暗号鍵を利用するアルゴリズムを使用することができる。復号鍵は暗号鍵から生成40することができ、次いで復号鍵は、暗号化した構成データを供給することが意図されるフィールド・プログラマブル・ゲート・アレイの不揮発性メモリに埋め込むことができる。

【0015】本発明の第3の態様によれば、フィールド・プログラマブル・ゲート・アレイを再構成する方法が提供される。この方法は、暗号化された構成データをフィールド・プログラマブル・ゲート・アレイに入力し、暗号化された構成データを復号し、および復号した構成データを配信してフィールド・プログラマブル・ゲート50

6

・アレイを構成することを含む。本発明のこの第3の態様では、復号ステップは、フィールド・プログラマブル・ゲート・アレイ内に不揮発性の形で記憶された復号鍵をアルゴリズムのオペランドとして使用して、暗号化された構成データに復号アルゴリズムを適用することを含むことができる。復号アルゴリズムは、ステートフルまたはステートレスとすることができる。

【0016】本発明の第4の態様によれば、外部から入力された暗号化された構成データに従って構成できるフィールド・プログラマブル・ゲート・アレイが提供される。ゲート・アレイは、復号鍵と共にロードされる不揮発性記憶素子を有し、また、構成データ入力チャネルの一部をなすデータ操作素子であって、復号鍵に応答して、入力チャネルを通過する構成データに復号アルゴリズムを適用するように構成されるデータ操作素子も有する。

【0017】さらに、フィールド・プログラマブル・ゲート・アレイ・モジュールも提供でき、このモジュールは、フィールド・プログラマブル・ゲート・アレイならびに不揮発性構成データ・メモリを含み、このフィールド・プログラマブル・ゲート・アレイおよびそのメモリは、構成データ転送リンクによって相互接続される。

【0018】本発明の代替実施態様では、デフォルト状態を有し、構成データによってプログラム状態に構成可能である構成可能論理構造と、暗号化された構成データを受け取るための入力端子と、プログラム状態を決めるための構成データのセットを記憶するためのデータ記憶域とを含むフィールド・プログラマブル・ゲート・アレイが提供され、構成可能論理構造は、デフォルト状態で、入力端子から受け取った暗号化された構成データを復号するように、かつ、復号した構成データを、続いて構成可能論理構造をプログラム状態に再構成するためにデータ記憶域に出力するように働く。データ記憶域は複数の構成データ保持レジスタを含むことができ、構成可能論理構造による復号の完了を検出するように、かつ、データ保持レジスタをトリガして、データ記憶域に記憶された構成データを構成可能論理構造にロードするように接続される状態機械を備えることもできる。

【0019】したがって、本発明の上記の実施態様および態様によれば、FPGA製造業者によって設計された論理構造と、FPGAアプリケーション設計者によって特定のアプリケーション用に開発された構成データの両方の点で、FPGA設計に組み入れられた知的財産および機密情報の安全性を高めることが可能である。復号すなわちスクランブル解除の回路がFPGAの内部に配置され、FPGAの外部からそれらに供給された構成データに作用する。したがって、FPGAに供給される構成データは、FPGAを使用する外部回路に対して暗号化された形でFPGAの外部に記憶される。したがって、例えばFPGAに電源投入する間に傍受することによ

7

て、構成データを入手することは、スクランブルされない生の形の構成データではなく暗号化された構成データを見ることになる。したがって、暗号化された構成データとFPGAの論理設計との関係を確立する作業を、より一層困難なものにすることができる。というのは、この関係が暗号化によって、より透過性の低いものにされるからである。さらに、同じ生の構成データが複数のFPGAにプログラムされる場合でも、異なるFPGAに異なる暗号化を使用することができ、したがって、傍受した構成データの変換処理は、依然として難しいものにされる。

【0020】本発明の一実施態様では、アプリケーション設計者は、復号プロセスの少なくとも1つの態様を定義する責任を負う。以下にさらに述べるこの実施態様では、設計者は復号鍵を定義する。設計者によって定義された鍵をオペランドとして使用する復号アルゴリズムは、FPGA製造業者によって予め決められ、通常、FPGAハードウェアに埋め込まれることになる。対応する暗号鍵および暗号化アルゴリズムもまた定義される。対応する暗号鍵と復号鍵は、同一でも異なるものでもよい。

【0021】ある手法では、FPGAに入力端子が備わり、これを通してアプリケーション設計者は、FPGA内の不揮発性メモリに鍵を入力することができる。この実施態様では、後に鍵が未許可でアクセスされるのを防ぐために、鍵の不揮発性メモリへの以後の外部アクセスをディスエーブルにするための構造も備わることが好ましい。例えば、鍵入力端子は、ディスエーブル信号にตอบสนองするように製造することができ、このディスエーブル信号は、受け取られると、復号鍵への以後の外部通信が閉鎖されるようにFPGA中で不可逆的な変更を引き起こす。

【0022】別の手法では、アプリケーション設計者がそれにより鍵の不揮発性メモリを外部からプログラムできる入力端子はない。その代わりに、アプリケーション設計者は、FPGA製造業者に所望の鍵を通知し、製造業者は、製造プロセスの一部としてその鍵を埋め込む。

【0023】最初に述べた手法には、アプリケーション設計者だけに知られることが必要な鍵情報に関する安全性が向上する利点がある。2番目に述べた手法には、FPGAがその不揮発性鍵メモリに外部からアクセス可能なチャンネルを有しない利点がある。

【0024】アプリケーション設計者には、アプリケーション設計の完了後、暗号化された構成データ・セットを生成する作業、すなわち暗号化されていない生の構成データから暗号化された構成データを生成する作業を与えることができる。このためにアプリケーション設計者は、設計ツールと共に、前述の復号鍵に対応する暗号鍵を使用することになり、この設計ツールはFPGA製造業者から提供することができ、この中には、FPGAに

8

埋め込まれた復号アルゴリズムの逆関数を含む暗号化アルゴリズムがプログラムされる。この設計ツールは、ソフトウェアまたはハードウェア・ベースとすることができる。

【0025】構成データが暗号化された形で記憶され、また暗号化された形で電源投入中にFPGAに転送されるため、リバース・エンジニアリングに対するバリアが設立される。クローニングが試みられる場合、侵害者は、どのように暗号化および復号化が構成されているかを知る必要があるが、この情報をFPGAから得ることは、極端に困難になると思われる。FPGAハードウェアのリバース・エンジニアリングは、設計者によって定義された復号データを記憶するのに使用される不揮発性記憶素子をFPGAチップの方々に点在させることにより、より一層難しくすることができる。このようにして素子を分散させる技術は、安全なマイクロコントローラ設計の技術分野から知られるが、この場合、ROM素子は分散され、あるいは空間的に点在させられ、したがって、これらは、次いで自動的に走査される可能性のある規則的かつ認識可能なパターンを形成しない。

【0026】本発明をよりよく理解できるように、かつ、本発明がどのように実行されるかを示すために、本発明を添付の図面を参照しながら例によって以下に述べる。

【0027】

【発明の実施の形態】図1は、フィールド・プログラマブル・ゲート・アレイ（FPGA）1、およびメモリ4の形をとる関連の構成データ記憶域の概略ブロック図である。FPGA1は、プログラマブル・ゲート・アレイ構造を含む機能部分3を含む。プログラマブル・ゲート・アレイ構造は、例えばM×Nアレイの構成可能論理ブロック（CLB）（図示せず）を含む。FPGA1は、通信リンク9を介して構成データ・メモリ4に接続され、この通信リンク9は、一方で構成データ・メモリ4の出力端子7に、他方でFPGA1の入力端子に接続される。

【0028】FPGA1はまた、論理5およびメモリ6の形をとる構成データ復号回路を含む。復号回路は入力端子8と復号回路の入力端子との間に伸びる通信リンク10を介して受け取った構成データに復号プロセスを適用する。復号回路はまた、機能部分を構成するように通信リンク11を介してFPGAの機能部分3に、復号した構成データを出力するための出力端子も含む。

【0029】メモリ6は、復号鍵を記憶する働きをし、論理5は、復号鍵をアルゴリズムのオペランドとして使用して、構成データに復号アルゴリズムを適用するように構成される。オペランドを定義する鍵データは、メモリ6から通信リンク16を介して論理5にロード可能である。復号鍵記憶域6は、EEPROM技術すなわちE²PR²OM技術に基づく不揮発性素子で形成される。あ

9

るいは、不揮発性素子は、フラッシュ・メモリ、ヒュージブル・リンクPROM、UV-EPROM、OTPROM、強誘電体セル、レーザ・プログラマブル・ヒューズ、または、FPGA中の他の場所で使用される技術と互換する他のどんな適した技術にも基づくことができる。技術の複数の組合せを単一のFPGA中で使用することもできる。

【0030】不揮発性復号鍵記憶域6には、製造段階か製造前のいずれかに、図1に破線で示す復号鍵入力端子13を介して復号鍵がロード可能である。FPGAはまた、ヒュージブル・スイッチの形をとるディスエーブル化素子14も含むが、この目的は、ディスエーブル化素子14が活動化された後で、復号鍵入力端子13から復号鍵記憶域6への外部通信を閉鎖することである。ディスエーブル化素子14は、復号鍵入力端子13に加えることのできるディスエーブル化信号の受領がディスエーブル化スイッチ中で不可逆的な変更を引き起こし、以後そのスイッチを永続的にオープン状態にするように、ディスエーブル化信号に応答する。この設計により、アプリケーション設計者は、復号鍵を復号鍵記憶域6にロードし、その復号鍵が首尾よくロードされたことを確認し、次いでディスエーブル化信号を復号鍵記憶域6の入力端子13に発行してディスエーブル化素子14を活動化させることができる。

【0031】FPGAの機能部分3は、SRAM技術に基づく揮発性素子で形成される。FPGAの機能部分3のSRAM技術は、一般に、不揮発性復号鍵記憶域6に使用されるEEPROM技術と互換できる。あるいは、他のFPGA構成要素、特に復号鍵記憶域6に使用される技術との互換性の要件を満たす他の技術を機能部分3に使用することもできる。

【0032】安全性をさらに高めるために、復号鍵メモリ6の不揮発性素子は、FPGAの機能部分3の揮発性素子の間に物理的に分散させられる。この手順により、物理的チップ配置は、よりリバース・エンジニアリングを受けにくいものになる。図5に、FPGAの各部、すなわち機能部分3、復号鍵記憶域6、および復号アルゴリズム論理5のチップ配置を概略的に示す。復号鍵記憶域6の不揮発性素子は、機能部分3の揮発性素子間のチップ配置にわたって分散させられている。複数の安全ビットを構成データ・メモリ・ブロックの領域にわたって分散させたプログラマブル論理デバイスは、Chiang他に譲渡された米国特許第5,349,249号に記載されており、この内容を参照により本明細書に組み込む。

【0033】FPGAに基づくシステムを設計するために、アプリケーション技術者は、FPGAの機能部分3をプログラムするための構成データを従来の方式で準備することになる。次いで設計者は暗号鍵を選択し、その暗号鍵を、設計ツールとして設計者が利用できる暗号

10

化アルゴリズムに入力する。次いで設計者は、自分が指定した暗号鍵を使用する暗号化アルゴリズムを適用して構成データを暗号化する。次いで暗号化された構成データは、設計者によって、不揮発性メモリまたは他のいずれかの適した記録媒体に組み入れることのできる構成データ記憶域4に記憶される。総称暗号化アルゴリズムは、FPGAの復号アルゴリズム論理5に組み入れられた復号アルゴリズムを形成する逆関数を有する。設計者指定の暗号鍵も対応する復号鍵を有し、これも再び、恒等関数とすることのできる逆関数によって結び付けられ、この復号鍵は、図1を参照しながら上にさらに述べたように、設計者によって直接、または設計者の要請で製造業者によって、FPGAの復号鍵記憶域6にロードされる。

【0034】図2に、設計者主導の構成データ暗号化プロセスを流れ図の形で示す。この方法は、ステップ20で構成データ・セットを入力し、次いでステップ21で、図1を参照しながら上にさらに述べた設計者指定の暗号鍵22をオペランドとして有する暗号化アルゴリズム23を構成データ・セットに適用することによって進行する。次いで、ステップ21で産出された暗号化された構成データ・セットは、ステップ24で、図1に示す構成データ記憶域4や中間記憶媒体などの記録媒体上に記憶される。

【0035】図3に、設計者主導によってFPGAの不揮発性復号鍵記憶域6に復号鍵を記憶することを概略的な流れ図の形で示す。このプロセスは、ステップ30で暗号鍵を入力し、ステップ31で暗号鍵から復号鍵を生成し、ステップ32でFPGAの復号鍵記憶域6に復号鍵を書き込むことによって進行する。

【0036】図4に、構成データ記憶域4からの暗号化された構成データで図1のFPGAを再構成する方法を流れ図の形で示す。再構成は通常、電源投入時に行われるが、いくつかの設計では実行中に行われることもある。暗号化された構成データは、ステップ40でFPGAに入力され、次いでステップ41で、暗号化された構成データに復号アルゴリズム43を適用することによって復号される。復号アルゴリズム43は、FPGAの復号鍵記憶域6に記憶された復号鍵42を使用する。復号された構成データは、ステップ44でFPGAの機能部分3内に配信され、それによりFPGAを構成する。復号アルゴリズム論理5に組み入れられる復号アルゴリズム43は、安全性をさらに高めるためにステートフルだが、より安全性の低いシステムではステートレスとすることもできる。ステートフルな復号アルゴリズムは、例えばリニア・フィードバック・シフト・レジスタ設計を使用するハードウェア中で実現することができる。

【0037】図6に、本発明の代替実施形態を示す。図1の実施形態の部分と同様の機能を有する部分に、同じ

参照番号を使用する。

【0038】先の実施形態のように、通信リンク9、出力端子7、および入力端子8を介して相互接続されるFPGA1および関連の構成データ・メモリ4を示す。FPGA1はまた、復号目的で鍵データを提供するために通信リンク16に接続された鍵データ・メモリ6も含む。

【0039】先の実施形態とは対照的に、専用の復号回路が備わるのではなく、FPGAの機能部分3および状態機械17中に復号機能が含まれる。状態機械17は、構成データのセットの復号が完了するのを検出し、それに応答してFPGAの機能部分3への通信リンク25上に出力を生成するように構成される。状態機械17の役割は、FPGAの機能部分3の設計に関する後続の考察を読めば、より容易に理解されるであろう。

【0040】図7に、機能部分3の構成可能論理ブロック(CLB)27および関連するレジスタの修正設計をより詳細に示す。機能部分3は、複数のCLB、例えばM×Nの二次元アレイをその中に含む。CLBは、通信リンク10から暗号化された構成データを、また通信リンク16から鍵データを受け取るように構成されている。

【0041】図7のCLB27に関連して、構成レジスタのセット18が存在する。従来のFPGA設計におけるように、構成レジスタ・セット18は構成データを保持する働きをし、この構成データは、CLB27にロードされたときにそのデータに従ってCLB27を構成する。

【0042】しかし、従来の設計とは対照的に、各CLBに保持レジスタのセット19も備えている。図7を参照すると、図示の保持レジスタ・セット19は、他の構成データのセットを保持する働きをする。保持レジスタ・セット19は、CLB27の出力端子から構成データを受け取り、それに記憶された構成データを構成レジスタ・セット18にロードするように接続される。図7で、レジスタ・セット18と19の間の接続は並列接続として示してあるが、直列接続とすることもできる。保持レジスタ・セット19はまた、状態機械から状態機械通信リンク25を介してトリガ信号を受け取るための入力端子も有する。さらに構成レジスタ・セット18は、グローバル・リセット信号を受け取るための入力端子も有し、この入力端子を介してリセット信号を受け取るとデフォルト状態を採用するように設計される。

【0043】デフォルト状態の構成レジスタ・セット18のコンテンツは、CLB27にロードされるときにFPGAを復号エンジンとして動作させ、したがって、通信リンク10を介して受け取られた暗号化された構成データは、通信リンク16を介して受け取られた鍵データに従って復号され、復号された形でCLB27から出力され、保持レジスタ・セット19に供給されて、そこに

記憶される。復号プロセスの完了は状態機械によって検出され、それに応答して、状態機械は通信リンク25に信号を出力する。この信号が保持レジスタ・セット19によって受け取られるとき、この信号は、保持レジスタ・セット19のコンテンツすなわち復号された構成データがメイン構成レジスタ・セット18に、次いでCLB27にロードされるようにし、次いでCLB27は、その復号エンジン状態から従来のFPGA動作のための所望のプログラム状態に状態を変更する。構成データのセットを2つ記憶することのできる構成メモリを有するプログラマブル論理デバイスは、Randy T. Ongに譲渡された米国特許第5,426,378号に記載されており、この内容を参照により本明細書に組み込む。

【0044】理解されたいが、図6および7の実施形態は、図1を参照しながらさらに述べたように、復号鍵入力端子およびディスエーブル化素子を含むように修正することもできる。

【0045】図6および7を参照しながら上に述べた代替実施形態は、チップ領域を減らして追加の復号機能を備えるために、デバイスの数を減らして実施することもできる。これは、FPGAの機能部分3が復号エンジンとして動作するような復号構成をデフォルトで採用するように、機能部分3を設計することによって達成される。

【0046】以上のことから、構成可能論理構造を有する機能部分と、機能部分を構成するための構成データを受け取るための入力端子と、構成データに復号プロセスを適用して、フィールド・プログラマブル・ゲート・アレイの機能部分を構成するために復号した構成データを生成するための手段とを含むフィールド・プログラマブル・ゲート・アレイを提供できることが理解されるであろう。復号手段は、復号鍵を記憶するための手段と、復号鍵をアルゴリズムのオペランドとして使用して構成データに復号アルゴリズムを適用するための手段とで構成することができる。従来の方式には、機能部分を構成するように、復号手段から復号された構成データを機能部分に配信する手段も存在する。

【0047】本発明の特定の実施形態を述べたが、添付の特許請求の範囲に定義する本発明の趣旨および範囲を逸脱することなく、多くの修正/追加、および/または代用を行うことができることを理解されたい。

【図面の簡単な説明】

【図1】本発明の実施形態によるフィールド・プログラマブル・ゲート・アレイおよび構成データ・メモリの概略ブロック図である。

【図2】フィールド・プログラマブル・ゲート・アレイ構成データを暗号化する方法を示す流れ図である。

【図3】図1のフィールド・プログラマブル・ゲート・アレイに復号鍵をロードする方法を示す流れ図である。

【図4】復号した構成データで図1のフィールド・プロ

13

グラマブル・ゲート・アレイを再構成する方法を示す流れ図である。

【図5】図1のフィールド・プログラマブル・ゲート・アレイのパーツのチップ配置を概略的に示す図である。

【図6】本発明の代替実施形態によるフィールド・プログラマブル・ゲート・アレイおよび構成データ・メモリの概略ブロック図である。

【図7】図6のフィールド・プログラマブル・ゲート・アレイの構成可能論理ブロック（CLB）および関連するレジスタの概略ブロック図である。

【符号の説明】

1 フィールド・プログラマブル・ゲート・アレイ（FPGA）

1 FPGA

3 機能部分

4 メモリ

4 構成データ記憶域

4 構成データ・メモリ

5 論理

6 メモリ

6 復号鍵メモリ

*6 復号鍵記憶域

6 不揮発性復号鍵記憶域

7 出力端子

8 入力端子

9 通信リンク

10 通信リンク

11 通信リンク

13 復号鍵入力端子

14 ディスエーブル化素子

16 通信リンク

17 状態機械

18 構成レジスタ・セット

19 保持レジスタ・セット

22 暗号鍵

23 暗号化アルゴリズム

25 通信リンク

25 状態機械通信リンク

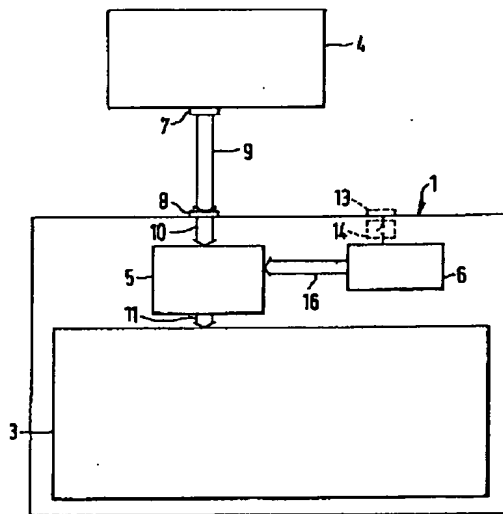
27 構成可能論理ブロック（CLB）

27 CLB

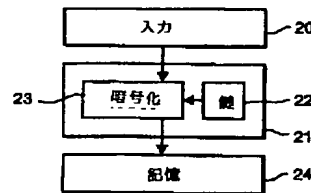
20 42 復号鍵

* 43 復号アルゴリズム

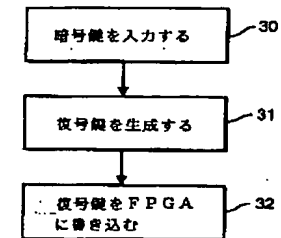
【図1】



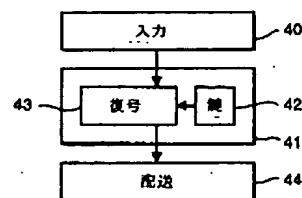
【図2】



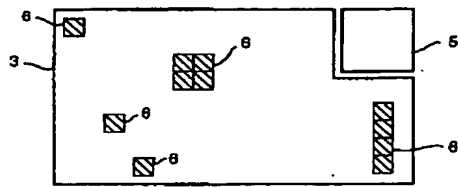
【図3】



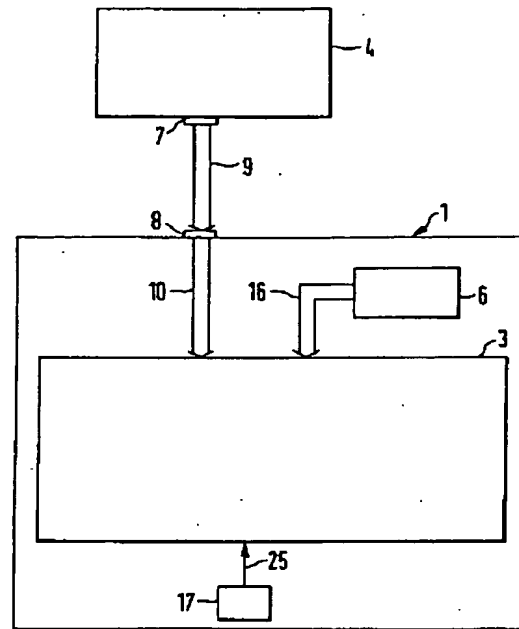
【図4】



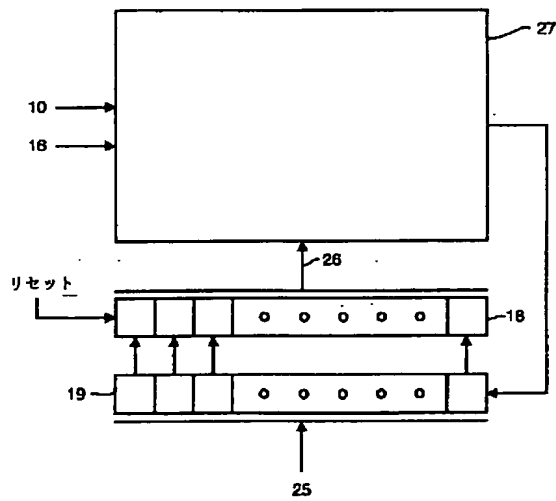
【図5】



【図6】



【図7】



フロントページの続き

(71)出願人 591064003

901 SAN ANTONIO ROAD
PALO ALTO, CA 94303, U.
S. A.

(72)発明者 ボール・ジェフリー・ガーネット
イギリス国・ダブリュエイ12 9 ビイダブ
リュ・マーシーサイド・ニュートンルー
ウィローズ・ザ ルークリー・2

Fターム(参考) 5B076 FA02

5J042 BA11 CA21 DA00

5J104 AA01 AA16 EA04 NA02 NA23